WE CLAIM:

1. A method for dynamically assessing threats to computers and computer networks using one or more security devices that generate events, comprising:

reading policy configuration information, wherein the policy configuration information comprises a global threat assessment event generation probability and one or more dynamic threat assessment rules comprising event probability information;

generating one or more abstract data types for each of the one or more dynamic threat assessment rules;

collecting and storing events from the one or more security devices in an event collection database;

reading each event in the event collection database;

determining if the each event is a member of each instance of the one or more abstract data types for each of the one or more dynamic threat assessment rules;

if the each event is a member of the each instance, adding the each event to the each instance and computing a probability of the each instance;

determining if the probability is greater than the global threat assessment event generation probability;

if the probability is greater than the global threat assessment event generation probability, generating a dynamic threat assessment event and placing the dynamic threat assessment event in the event collection database;

determining if the each event is a starting member of an instance of the one or more abstract data types for each of the one or more dynamic threat assessment rules; and if the each event is a starting member of the instance, creating the instance and adding the each event to the instance.

2. The method of claim 1, wherein the one or more security devices comprise an intrusion detection system, a network intrusion detection system, a host intrusion detection system, a router, a firewall, and a system logger.

3. The method of claim 1, wherein the policy configuration information further comprises rule probability thresholds.

4. The method of claim 1, wherein the policy configuration information further comprises event collection database configurations.

5. The method of claim 1, wherein the policy configuration information further comprises operation parameters.

6. The method of claim 1, wherein the one or more abstract data types comprise graphs, trees, lists, state machines, hash tables, and Bayesian networks.

7. The method of claim 1, wherein the probability of the each instance is computed based on one or more of the conditions comprising a number of other events, a type of the other events, an order of the other events, and a timing of the other events.

8. The method of claim 3, further comprising determining if the probability is greater than a rule probability threshold for the each instance.

9. The method of claim 8, further comprising if the probability is greater than the rule probability threshold for the each instance, generating a dynamic threat assessment event and placing it in the event collection database.

10. The method of claim 1, further comprising receiving and storing events from the one or more security devices in the event collection database.

11. The method of claim 1, further comprising removing the each instance from memory, if the probability is greater than the global threat assessment event probability.

12. The method of claim 8, further comprising removing the each instance from memory, if the probability is greater than the rule probability threshold for the each instance.

13. A system for dynamically assessing threats to computers and computer networks, comprising:

one or more security devices that generate events;

an event collection database, wherein the event collection database collects and stores events of the one or more security devices;

policy configuration information, wherein the policy configuration information comprises a global threat assessment event generation probability and one or more dynamic threat assessment rules comprising event probability information; and

a dynamic threat assessment engine,

wherein the dynamic threat assessment engine accepts the policy configuration information;

wherein the dynamic threat assessment engine generates one or more abstract data types for the one or more dynamic threat assessment rules;

wherein the dynamic threat assessment engine reads each event in the event collection database;

wherein the dynamic threat assessment engine determines if the each event is a member of each instance of the one or more abstract data types for each of the one or more dynamic threat assessment rules;

wherein if the each event is a member of the each instance, the dynamic threat assessment engine adds the each event to the each instance and computes a probability of the each instance;

wherein the dynamic threat assessment engine determines if the probability is greater than the global threat assessment event generation probability;

wherein if the probability is greater than the global threat assessment event generation probability, the dynamic threat assessment engine generates a dynamic threat assessment event and places the dynamic threat assessment event in the event collection database;

wherein the dynamic threat assessment engine determines if the each event is a starting member of an instance of the one or more abstract data types for each of the one or more dynamic threat assessment rules; and

wherein if the each event is a starting member of the instance, the dynamic threat assessment engine creates the instance and adds the each event to the instance.

14. The system of claim 13, wherein the one or more security devices comprise an intrusion detection system, a network intrusion detection system, a host intrusion detection system, a router, a firewall, and a system logger.

15. The system of claim 13, wherein the policy configuration information further comprises rule probability thresholds.

16. The method of claim 13, wherein the policy configuration information further comprises event collection database configurations.

17. The method of claim 13, wherein the policy configuration information further comprises operation parameters.

18. The system of claim 13, wherein the one or more abstract data types comprise graphs, trees, lists, state machines, hash tables, and Bayesian networks.

19. The system of claim 13, wherein the probability of the each instance is computed based on one or more of the conditions comprising a number of other events, a type of the other events, an order of the other events, and a timing of the other events.

20. The system of claim 15, wherein the dynamic threat assessment engine determines if the probability is greater than a rule probability threshold for the each instance.

21. The system of claim 20, wherein if the probability is greater than the rule probability threshold for the each instance, the dynamic threat assessment engine generates a dynamic threat assessment event and places it in the event collection database.

22. The system of claim 13, wherein the event collection database receives and stores events from the one or more security devices.

23. The method of claim 13, wherein the dynamic threat assessment engine removes the each instance from memory, if the probability is greater than the global threat assessment event probability.

24. The method of claim 20, wherein the dynamic threat assessment engine removes the each instance from memory, if the probability is greater than the rule probability threshold for the each instance.

25. The system of claim 13, wherein the event collection database comprises the logging system of a security device that generates events.

26. The system of claim 13, further comprising a management console comprising the event collection database, the policy configuration information, and the dynamic threat assessment engine.

27. A method for assessing a threat probability of an event generated by a security device, comprising:

receiving the event from the security device in an event collection database;

if the event matches an unpopulated member of an instance of an abstract data type that represents a rule that describes how events are combined to form a threat, adding the event to the instance and computing a probability of the instance; and if the probability is greater than a global threat assessment event generation probability,

generating a second event and placing the second event in the event collection database.